量子情報処理(第48回物性若手夏の学校(2003年度),講義ノート)

AUTHOR(S):

井元, 信之

CITATION:

井元, 信之. 量子情報処理(第48回物性若手夏の学校(2003年度),講義ノート). 物性研究 2004, 81(5): 722-732

ISSUE DATE:

2004-02-20

URL:

http://hdl.handle.net/2433/97752

量子情報処理

総合研究大学院大学　井元信之

量子情報処理は量子力学と情報通信が結婚して出来たミュータントともいうべき新しい分野である。これは量子力学の原理に基づくデバイスを使って現在のコンピューターや通信の速度を上げようという話ではなく、論理演算のあり方そのものが従来のものと異なり、量子力学の原理に基づく新しい方法である。そのために従来の情報処理や通信と質的に異なる、新しい情報処理や通信を可能にすることが理論的に明らかになって来ており、その絶大な潜在能力の故に最近にわかに注目されている研究分野である。このサブゼミではこの分野について概観することを目的とする。予備知識としては線形代数のみを仮定するが、量子力学の初歩的言葉使いも多少用いる。

0.イントロダクション

量子力学の原理として有名なものに不確定性原理がある。これは粒子の位置を測定すると運動量が不確定となり、その逆もしかりというものである。このような関係にある物理量は、粒子の位置と運動量、光の位相と光子数、x・y・zの3方向のスピン変数などいろいろな組合せがあり、それらは共役な物理量と呼ばれる。共役な物理量の一方に信号を載せ、他の物理量を読み出すと、元の信号は破壊される。この性質を利用して、正規のユーザー以外が預金を引き出そうとすると認証データが壊れて引き出せないような預金通帳のアイデアをWiesnerが1970年代の初めに提唱しようとした。このアイデアは長いこと論文掲載に至らず、人々の知るところではなかった。しかしそれにヒントを得たBennettとBrassardが1984年に量子暗号のアイデアを発表した。

一方、現在のコンピューターの能力- ある種の問題を解くプログラムがきちんと停止して答えを出すか、あるいはそこに至るまでの計算時間はどのくらいか- を調べるための理論的モデルとしてチューリングマシンが知られていたが、それに量子力学の原理を導入するとどうなるかという研究をDeutschは1985年に発表した。

以上の二つが量子情報処理分野の発端であるが、発端の後の数年間、量子暗号も量子コンピューティングも人々の注目するところではなかった。少数の人達が細々と理論構築をやっていたが、1990年になってEkertがその面白さ・可能性を人々に説いて回り、他の研究者の参入と本格的開拓が始まった。量子暗号では光通信による実験が行われ始め、また量子コンピューティングは現代暗号の主流である「公開鍵暗号」を理論上破る

ことが1994年にShorによって示された。公開鍵暗号を破るという驚くべき理論が発表されたインパクトは極めて大きく、この時から量子コンピューティングの重要性が一般に知られるようになった。また、量子コンピューティングによっても破られない暗号として量子暗号の重要性も認識されることとなった。

1．量子論の不思議

1.1 重ね合わせの原理

量子力学の根本は重ね合わせの原理に尽きる。しかしこの原理から現象論的に不思議な二つの性質が導かれる。一つは「クローン生成禁止定理」であり、もう一つは「エンタングルメント」と呼ばれる特殊な相関関係である。クローン生成禁止定理は別の見方をすると不確定性原理となり、この方が広く知られている言葉であろう。エンタングルメントは日本語訳が確定していないが、量子力学的「絡み合い」「もつれ合い」「量子相関」「連関状態」などと呼ばれる。ここでは、そのままで世界的に通用するエンタングルメント(entanglement)と呼ぶことにする。

重ね合わせの原理とは、物理系を一つ考えたとき（たとえば原子とか、ある空間の中の電磁場とか、スピンを持ったある粒子、あるいはそれらの複合体など）その系のエネルギーが確定したいくつかの状態- エネルギー固有状態- のどれかになっているというだけでなく、それらの重ね合わせも立派な一つの「状態」であることを謳っている。すなわち異なるエネルギー値に対応する状態をそれぞれ直交するベクトルとみなし、それらのベクトル合成を行って斜め方向を向いたベクトルを作ると、それも物理的に意味のある状態となる。さらに一般に、エネルギー以外に任意の物理量に対する固有状態やその重ね合わせも状態になり得る。これらのベクトルが張る空間は線形空間となるが、それをヒルベルト空間と呼ぶ。たとえば二準位原子では基底状態と励起状態が直交基底となる二次元の線形空間をなす。光では光子数が０、１・・・というエネルギー状態に対応して無限次元となる。一光子の偏光だけを考えると、これは２次元である。

重ね合わせ状態と確率的混合状態は全く別物なので区別されなければならない。たとえばエネルギーが基底状態にある原子と励起状態にある原子が同数混ざった原子集団からランダムに原子一つを取り出すと、その一つの原子の状態は基底状態 50% と励起状態 50% の混合した状態と解釈する。エネルギーを観測すると、基底状態か励起状態のどちらかであることが分かるが、これは初めから決まっていたのを見ただけであり、見る前は「混合した状態(mixed state)」にある。

重ね合わせ状態はこれとは異なる。基底状態ベクトルと励起状態ベクトルを $1/\sqrt{2}$ の振幅で足し合わせた状態は重ね合わせ状態であるが、これは「基底状態か励起状態か初

めから決まっているが知らないだけ」という状態ではない。観測すれば確率50%で基底状態か励起状態かが観測されるという点では同じだが、そのような重ね合わせ状態は他にも$+1/\sqrt{2}$と$-1/\sqrt{2}$で足したものとか（位相が180度逆）、$+1/\sqrt{2}$と$i/\sqrt{2}$(位相が90度)で足したものなど無限にある。位相情報を明確に保持しているのが重ね合わせ状態で、これを純粋状態(pure state)という。これに対し、位相情報を忘れた状態が混合状態である。

最もわかりやすいのは光子一つの偏光状態で、縦偏光の光子と横偏光の光子が半々に混ざった箱から一つ取り出した光子の状態と、＋45 度傾いた純粋な直線偏光の光子は明らかに別の状態である。前者は「縦か横か決まっているのだが見る前は確率が半々ということしか知らないだけの状態」であるが、後者を「縦か横か決まっている」とは言わないことは明らかである。縦か横が確率半々で観測される純粋状態としてはこの他に－45度傾いた偏光(位相が逆)や円偏光(位相が90度)など無限にある。このため重ね合わせ状態は位相を指定することが本質的である。

1.2 量子観測とクローン生成禁止定理

エネルギー固有状態に対応する直交基底と別に斜め方向に向いた直交基底をとることができるが、その新たな基底に対応する物理量はもはやエネルギーではない何かである。それが何であるかは個々の系に依存する。ヒルベルト空間の中で純粋状態は一つの状態ベクトルで表されるが、その状態のもとである物理量を観測するということは、その物理量の固有ベクトルのどれかに射影することを意味する（射影公理)。どの固有ベクトルに射影されるかは全く確率的現象であり、特定の固有ベクトルに射影が起こる確率はそのベクトルと状態ベクトルの内積の絶対値の二乗となる（Bornの確率解釈)。

二つの物理量のそれぞれが張る直交基底が斜め同士の関係にあるとき、その二つの物理量の同時観測は両立しない。なぜならエネルギー固有ベクトルへの射影を行って次に新たな基底への射影を行うことと、その順序を換えたものの結果が異なるため、最初に行った観測が次に行う観測に影響を与えてしまうからである。これを一般化すると「交換しない物理量－ すなわち互いに共役な物理量－ は同時に確定することはできない」ことになる（不確定性原理)。「交換しない」とは物理量に対応する演算子（行列）が二つの物理量について交換しないという意味である。

クローン生成禁止定理(no-cloning theorem)とは「未知の量子状態にある物理系のクローンを作ることはできない」という定理である。これはたとえば、特定の偏光状態にある光子一つを誰かが発生し、その偏光状態が何であるか教えられずに光子だけを我々がもらったとき、同じ偏光状態にある光子を（元の光子を壊さずに）別に生成することはできない、ということを言っている。仮にクローン生成ができると、元の光子の縦横偏光を測定し複製光子の円偏光を測定することができるので、「両者の同時測定はでき

ない」ことに反する。

ただし既知の状態にある物理系のクローンはいくらでも作れることに注意されたい。そうでないと再現性のある物理実験はできない。たとえば22.5度傾いた直線偏光の光子を大量に作りたければ、いくらでもできる。

1.3 エンタングルメント

系が二つ以上ある場合を考える。例えば光子が二つある場合、偏光状態としては縦縦、縦横、横縦、横横の４種類があり、これらの重ね合わせも許されるので、４次元のヒルベルト空間を考える必要がある。これは２次元＋２次元で４次元になったのではなく２×２＝４次元である。一般に系１がｎ次元、系２がｍ次元、系３がｋ次元・・・のとき、全体系のヒルベルト空間の次元はｎ＋ｍ＋ｋ＋・・ではなく、ｎ×ｍ×ｋ×・・となる。基底の数を考えればこれは明らかである。ここでは簡単のため光子二つだけを考える。ディラックの記法にならい、四つの状態ベクトルを｜縦縦〉｜縦横〉｜横縦〉｜横横〉と書くことにする。ベクトルｘはｘの上に→をつけるのが一般的だが、この｜ｘ〉という記号の方がはるかに便利である。｜ｘ〉は列ベクトルで〈ｘ｜が行ベクトルに対応すると思えばよい。この場合内積〈ｘ｜ｙ〉は複素数となり、ディアディック｜ｘ〉〈ｙ｜は行列に対応する。

二光子（離れていてもよい）を一つの系と見て｜ϕ^-〉≡｜縦横〉－｜横縦〉という状態を考えてみる。これは左の光子が縦偏光なら右は横偏光、逆なら逆、という状態を位相180度でベクトル合成したものである。この状態にある光子をどんなに離したとしても、左の光子が縦と測定されたら瞬時に右は横と結論される。しかしこれだけでは不思議ではないだろう。夫婦がたまたま非常に離れた場所に旅行したとき、片方が女とわかれば瞬時にもう片方は男であることが結論されるのと同じである。

不思議なことは基底を変えたときに起こる。線形空間はどんな正規直交基底を取ってもよいので、状態｜ϕ^-〉を縦横基底でなく＋45度と－45度の偏光の基底で表してもよい。また右回り円偏光と左回り円偏光で表してもよい。これをやると、状態｜ϕ^-〉は｜＋－〉－｜－＋〉となったり、｜右左〉－｜左右〉となることがわかる。これは何を意味するか？　どんな偏光を測っても、左の光子と右の光子は逆になっているということである。すなわち、どんな偏光も完全な(負の)相関があるということである。これは「異なる偏光の同時確定はできない」ことを思い出すと不思議である。どの偏光が測定されるかわからないのに、特定の偏光が測定されたことを、離れた所に居るもう一つの光子はどうやって知るのか？　またこの二光子状態は、たまたま逆の偏光を持つ確定状態の光子を独立に寄せ集めたのではなく、片方の経験が瞬時にもう一方に伝わるという意味で、背後の世界で繋がりを持ったクローンのような状態である。この｜ϕ^-〉のような状態のことをエンタングルした状態と呼ぶ。

ここでよく考えてみると、上記のことを不思議だと思えるのは、量子力学すなわち不確定性原理あるいはクローン禁止定理を知っているからである。量子力学を知らなければ、あるいは量子力学は間違っているかもしれないと考えると、もともと一つの光子に「円偏光が測定された場合にはこれこれの値を出し、直線偏光ならこれこれの値・・・」という属性が記録されていると考えてどこが悪いのだろうか？　この考え方は「隠れた変数の理論」と呼ばれる。上記の相関はこの理論でも説明できてしまうので、そう考えると不思議ではない。エンタングルメントは不思議だということを説明するのに量子力学の常識を前提としてはならない。

この「隠れた変数」（つまり各光子に書き込まれている情報）の影響は光速以上の速度で伝わることはないと仮定するのが自然である。そうでなければ相対性理論に反する。この前提のもとに論理的に予想されることと反する実験結果はないはずである。ところが、うまく工夫した実験を行うと、そのような実験結果が出るのである。詳細は講義で説明するが、これは量子力学を仮定する以前に認識される矛盾なので、極めて不可解な現象である。なぜ不可解と思われるか、その前提となった思いこみをもう一度書くと、

(1) 同じ状態に準備した系のコピーに何度行っても同じ測定結果が出る場合、その値はもともとその系に書き込まれていた属性を反映している。

(2) その属性は光速を超えて他の系に伝わることはない。

(3) 組合せ実験系での結果を予測するときに用いる論理的推論は正しい。

である。どこにも量子力学はない。このうち少なくとも一つは間違いであることを実験結果は意味している。このうち(3)は明らかに正しいと考えられる。(1)もほとんど言葉の定義である。そこで何らかの形で(2)が間違っていると結論される。これは何か新しい遠隔相関のあり方が自然界に存在することを意味する。この前提(2)を相対論に矛盾しない形で書き換えることは可能であろうか？

その答(の少なくとも一つ)が量子力学であり、その新しい遠隔相関のあり方はこれまでにない概念なので新しい名前をつける必要がある。それがエンタングルメントである。

2. 計算・暗号・多者間プロトコル・通信

量子情報処理が古典情報処理にできないことができる、ということを見るためには、まず古典情報処理の例と限界について知る必要がある。ここではその最小限の解説をする。多者間プロトコルと通信については講義で説明するので、ここでは暗号と素因数分解について解説する。

2．1　暗号

暗号とは、送信者（アリスと呼ぼう）が受信者（ボブと呼ぼう）にメッセージを送るに際し、盗聴者（イヴと呼ぼう）に中身を見られずに送る方法である。最も簡単なもの

は、アリスとボブで共通の乱数表（鍵と呼ばれる二進数）を共有しておいて、アリスはメッセージを二進数で表し、それと鍵の間で演算（たとえば排他的 OR、同じことだが足して2で割ってあまりを出す）を行う。このようにして変換された暗号文（二進数列）はあらたな乱数になっており、イヴが盗聴しても意味不明である。ボブは受け取った暗号文と鍵の排他的 OR を再びとることにより元のメッセージが復元される。この方式は「秘密鍵暗号」あるいは「非公開鍵暗号」と呼ばれ、鍵を使い捨てにすれば絶対的安全性が保障される。この暗号の問題点はいかにして鍵そのものを安全にアリスとボブの間で配送するかという点にある。

この「鍵の配送」が不要な暗号が考案されている。これは「公開鍵暗号」と呼ばれ、現代暗号の基礎となる暗号である。これは施錠専用鍵と解錠鍵が別であり、まず受信者ボブがこの両方の鍵を作り、施錠専用鍵を公開し、解錠鍵は自分で保管する。アリスは公開された鍵を使って暗号文を作りボブに送る。この暗号文が盗聴されたとしても、読めるのは解錠鍵を持っているボブだけとなる。

ステップ１：ボブは施錠鍵 e と N それに解錠鍵 d を次のようにして作成し、e と N だけ公開する。

(1) 二つの大きな素数 p と q を適当に選択し、N = pq を計算する。

(2) p-1 と q-1 の最小公倍数 L を計算し、L と互いに素で L より小さい数から適当に e を選択する。

(3) ed を L で割ると 1 になるような数 d を探す。これを式では ed = 1 (mod L) と書く。

ステップ２：アリスはメッセージを整数で表した P(plain text の略)から暗号文 C を $C = P^e \pmod N$ により計算する。

ステップ３：ボブは受け取った暗号文 C から元のメッセージを $P = C^d \pmod N$ により計算する。

最後のステップ３でなぜ元の整数 P が復元するかは省略するが、この暗号がどうして安全性かを考えてみる。まず N の素因数分解が簡単にできるようであれば p と q がすぐわかってしまうので、第三者が解錠鍵 d を知ってしまう。またステップ 2 の(mod N)の付いた指数関数の逆演算（離散対数と呼ぶ）が簡単にできるようでは、解錠鍵 d を知らなくてもメッセージ P がわかってしまう。したがってまず素因数分解や離散対数が「事実上できないほど難しい問題」でなければならない。また逆に、上記ステップで使われる計算はすべて「実際にすぐできる簡単な問題」でなければならない。そして次に述べるように実際そのようになっている。

２．２　簡単な問題と難しい問題

「簡単な問題」や「難しい問題」とは何か？　それは以下のように定義する。たとえば $11\times41\times73\times101\times137\times271\times3541\times9091\times27961\times1676321\times5964848081 = 1111111111111111111111111111111111111111$ というかけ算を考える。左辺から右辺は紙の上での筆算でもすぐできる。しかし右辺から左辺の素因数分解は非常に時間がかかる。この例は 40 桁の数の素因数分解だが、少し桁数を増やして Mathematica か何かで実験してみればすぐわかる。かけ算と素因数分解は同じ数の別の表現を移し替える逆の問題であるにすぎないが、素因数分解の方がずっと手順がかかる。左辺の桁数を倍にしたときかけ算はせいぜい $2\times2=4$ 倍程度だが、右辺の桁数を倍にすると、10 の何十乗倍も時間がかかる。

このように「問題のサイズを n 倍したとき解くための基本演算ステップ数が n の多項式以内でしか増えない」問題を易しい問題(P 型問題)と呼び、「問題のサイズを n 倍したとき解くための基本演算ステップ数が n の多項式で書けないほど(典型的には指数関数的に)急速に増加する」問題を難しい問題(P 型でない問題)と呼ぶ。この区別は理論的に次のような便利さがある。すなわち、易しい問題を多項式個組み合わせても依然として易しい問題にとどまり、難しい問題に転化されない。別の言い方では「易しい問題」のサブルーチンを多項式個含むタスクはやはり「易しい問題」である。

素因数分解以外に「難しい問題」の例としては、離散対数、巡回セールスマン問題などが知られている。このうち素因数分解と離散対数は量子コンピューティングにより「易しい問題」に転化されることが原理的にわかっているが、巡回セールスマン問題も量子コンピューティングで多項式時間以内に解けるか否かはわかっていない。

次に量子コンピューティングの布石として、「確定的計算」と「確率的計算」について述べる。計算機が全く同じ計算を繰り返すようなアルゴリズムを確定的アルゴリズムと言い、これに対し乱数を引くプロセスを含むようなものを確率的アルゴリズムと言う。確率的アルゴリズムのプログラムをランさせると毎回違った計算プロセスを踏むが、同じ答に到達するはずである（きちんと設計されたプログラムなら)。確率的アルゴリズムの方が確定的アルゴリズムより広範囲の問題を解くことができることが知られている。

２．３　確率的素因数分解

この確率的アルゴリズムを使った素因数分解の方法を示そう。もちろんこの方法で素因数分解が「易しく」解けるなら量子コンピューターは要らないので、そうではないが、量子コンピューティングによる素因数分解はこの方法を使うのである。いま、

N：与えられた（何百桁もの非常に大きな）整数、

m：乱数表を振って選ばれた（小さな）整数、
n：整数列 0, 1, 2, ・・・

として、素因数分解の手順は次のようになる。

ステップ１： 数列F(n) ≡ m^n (mod N) を作れ
（ここでmod N とは N で割った余りを求める計算である。ステップ１はべき乗譲与計算と呼ばれる。）
ステップ２：数列F(n)は周期関数となるので、F(n+r) = F(n)となる周期r を求めよ。
ステップ３：Nと $m^{r/2}$＋１のGCD（最大公約数）およびNと $m^{r/2}$－１のGCDを求めよ。
ステップ４：それは高確率でNの約数になっているので、わり算して確かめよ。
OKならさらに割って行く。だめなら違うmを選び初めから繰り返せ。

以下に実例を示す。Nとして本当に巨大整数をとるわけに行かないので、N=15としておく。また、乱数を引いた結果 m＝２となったとする。

ステップ１：F(0) = 1
F(1) = 2
F(2) = 4
F(3) = 8
F(4) = 1
F(5) = 2
・・・
ステップ２：r = 4
ステップ３：$m^{r/2}$±１ = 5, 3
GCDを求めるまでもなくこれは15の約数
計算終了

上記ステップ1、2、3のうち少なくとも一つ「難しい問題」の部分があるはずである。それはステップ２である。量子コンピューティングはこのステップ２を量子力学の原理を使って易しい問題に転化しようというものである。

３．量子計算・量子暗号

量子情報処理を使った素因数分解と（秘密鍵暗号方式における）鍵配送について述べる。講義では他に量子多者間プロトコルや量子テレポーテーションについて解説する。

３．１　基本演算素子

現在のコンピューターがAND、OR、NOTの基本素子があれば組み立てられることはよく知られている。このうちNOTは１入力１出力素子、ANDとORは２入力１出力素子である。量子情報処理についてもこのような基本演算素子がある。ただし量子力学では演算はユニタリー演算子で表されるので、素子は可逆でなければならず、入力数と出力数は等しくなければならない。

１入力１出力の基本素子にはアダマール変換などがある。また２入力２出力の基本素子には制御NOTなどがある。これらの詳細は講義に譲るが、要は、これらの基本素子で必要な演算が全て組み立てられる。その基本素子の数が問題のサイズに対して多項式個で済むか指数個必要かということが重要である。

３．２　量子暗号

量子暗号は秘密鍵暗号方式における鍵配送に用いる。例としてBB84と呼ばれる量子暗号を解説する。光子一つひとつの偏光に０と１をコーディングする変調法として縦／横と＋45／－45度の二種類の直線偏光を用いる。

ステップ１：元になる乱数表を見ながら送信者は１ビットごとにランダムに縦横変調か斜め変調を選び、光子を送信する。ただし光子送信のタイミング以外の情報は公表しない。

ステップ２：受信者も独立に縦横復調か斜め復調を選び光子を受信する。

ステップ３：事後に送信者と受信者は古典的別回線でそれぞれの選択を公開し、両者の選択が一致した約半数の測定結果をそれぞれ保管し、一致なかった残りのビットは捨てる。盗聴者がいなければこれだけで同一乱数表の発生が可能である。

ステップ４：盗聴痕跡を検出するため、保管しているビットの中から適当数のビットを合議の上ランダムに選んでテストビットとし、その測定値まで確認する。盗聴があれば一つのテストビットにつき0.25の確率で測定値の不一致が発見される。言い換えると、0.75の確率で盗聴者を逃す。そこで、危険率εに対し$N = \log\varepsilon/\log(0.75)$個をテストビットとすることにより、設定した任意の危険率でしか盗聴者をのがさないようにできる。

ステップ５：テストの結果測定不一致のなかった乱数表は危険率ε以下で「盗聴痕跡のない鍵」として採用する。

実際は伝送路や装置が完全な量子通信路や量子観測器でないため、もう少し複雑な手順

をとるが、基本的にはこれで共通の乱数を秘密に持てるので、あとはこの乱数でメッセージを暗号文に変換し、通常の通信で送受する。

３．３　量子コンピューティングによる素因数分解

２章３節の確率的素因数分解を思い出すと、数列を書き下すためには整数ｎとその関数Ｆ(n)を格納する演算レジスターが必要である。そのためＭ（＞ log N）個の二準位系（量子ビット）から成る演算レジスター二つを用意する。レジスター１にはｎを格納し、レジスター２には最終的にＦ(n) を格納する。下記で左のベクトルがレジスター１の状態を、右のベクトルがレジスター２の状態を表す。二進数表現のため、０や１はそのまま量子ビットの状態を表す。まず初期状態としてはいずれのレジスターも絶対零度状態とする。すなわち

$$\text{初期状態} = |0\cdots000\rangle \times |0\cdots000\rangle$$

次にレジスター１のみ、全ての量子ビットにアダマール変換を施す。すなわち

$$\begin{aligned}\text{アダマール変換後} = \Sigma |n\rangle \times |0\rangle = {} & |0\cdots000\rangle \times |0\cdots000\rangle \\ & + |0\cdots001\rangle \times |0\cdots000\rangle \\ & + |0\cdots010\rangle \times |0\cdots000\rangle \\ & + |0\cdots011\rangle \times |0\cdots000\rangle \\ & \cdots \\ & + |1\cdots111\rangle \times |0\cdots000\rangle\end{aligned}$$

全ての項でレジスター２は絶対零度状態なので、これはレジスター１と２の状態の単なる積であるから、もちろんエンタングルしていない状態である。次にべき乗剰余計算を行う。和（Σ）の項数がＭに対し指数的であるにもかかわらず、これが多項式時間以内にできることが理論的にわかっている。それは下記一般項の形を見ると $i_1, i_2, \cdots, i_M$ で条件付き判断を行えばよい形になっていることからも分かる。

$$\begin{aligned}\text{べき乗剰余計算後} = \Sigma |n\rangle \times |m^n \bmod N\rangle \\ = {} & |0\cdots000\rangle \times |1 \bmod N\rangle \\ & + |0\cdots001\rangle \times |m^1 \bmod N\rangle \\ & + |0\cdots010\rangle \times |m^2 \times 1 \bmod N\rangle \\ & + |0\cdots011\rangle \times |m^2 \times m^1 \bmod N\rangle \\ & \cdots\end{aligned}$$

$$+|1\cdots111\rangle \times |m^{q-1} \bmod N\rangle$$

(エンタングルしている)

$$\text{一般項}=|i_{q-1}\cdots i_2 i_1 i_0\rangle \times |(m^{2^q})^{i_q}\ldots(m^{2^2})^{i_2}(m^{2^1})^{i_1}(m^{2^0})^{i_0} \bmod N\rangle$$

以上で2.3で述べたステップ1が実行される。

次にレジスター2は（nに対し）周期的に同じ状態をとるようになっているはずなので、「量子状態のフーリエ変換」を行ってやれば、その周期の値に関係する整数番目の状態のみ量子干渉によって強め合う。ここで量子状態のフーリエ変換とは、普通のフーリエ変換が変数xに対する関数f（x）のフーリエ変換を定義するのと同様に、変数レジスター1に対する関数レジスター2のフーリエ変換として定義される。このフーリエ変換も多項式時間以内で行えることが理論的に分かっている。そこでレジスター1について量子観測を行うと、周期rに関係する答えが高い確率で得られる。以上でステップ2が実行される。

ステップ3は量子的でなく2.3節と同様通常計算で行えばよい。以上により全てのステップが多項式時間以内で行えることになる。

4．おわりに

講義ではさらに研究の現状や最近の進展について解説する。この若い分野が多くの人の興味を引き、未解決問題の解明とともに新しいアイデアの創出が一層行われて行くことを願う。

参考文献

・井元「量子工学」imidas'02, 47-52 (2003).
・A. Miranowicz、玉木「量子テレポーテーション」数理科学第40巻第11号(2002).
・井元「量子力学の解釈問題」数理科学第40巻第7号(2002).
・小芦「量子暗号とその背後にある原理」数理科学第39巻6号 (2001).
・井元・小芦「量子暗号と量子論」日本物理学会誌第56巻1号 (2001) .
・井元「量子コンピューティング」 日本物理学会編「アインシュタインとボーア」裳華房(1999年).